AU/ACSC/WANDMACHER/AY10

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

The U.S. Needs International Cyber Treaties

by

James T. Wandmacher, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisors: Mr. Roger Philipsek and Lt. Col Mark Black

Maxwell Air Force Base, Alabama

March 2010

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

The United States did not wait for a nuclear attack on it's soil before pursuing international treaties on nuclear weapons. Nor should it wait for a catastrophic cyber attack. Both history and exercises have demonstrated the world cannot afford to wait any longer. Cyber attacks have occurred for years and threaten to impact nations in many ways from simple denial of access to destruction of infrastructure. Examples of the threats abound from crippling attacks against Estonia, to ongoing espionage attributed to China, and exercises like Cyber Storm and Cyber ShockWave. In the past nations have signed treaties that established law regarding land, air, and sea domains, to regulate warfare, and halt arms races to avoid catastrophic consequences to populations. It is time to overcome such obstacles to international agreement as definitions, attribution, and compliance. Agreements can start with a compromise in defining what constitutes attacks and grow on the international cooperation already present in the UN and NATO. In the past governments have acted to ensure peace for their populations as well as established international laws for the conduct of war. It is time for the international community to include this advance in warfare into those laws.

The threat of cyber warfare is not new. For several years, nations have been aware of the potential damage of cyber attacks. Some international organizations have already formed to deal with issues surrounding cyber warfare. However, no major treaties between nations exist regarding this form of combat. Examining the history of cyber warfare, the inadequate international response, the obstacles to international agreement, and poor U.S. readiness demonstrates the current need for the U.S. to lead the effort to codify treaties.

First, a brief history of cyber warfare helps to shed light on the international dilemma. Many people are aware of the 2007 cyber attacks on Estonia.[1] Estonia accused Russia for the crippling of their networks. But the president of the Cyber Defense Agency said it's only the "tip of the iceberg of the quantity and quality of attacks that are going on."[2] He notes that other nations, including Israel, India, Pakistan, the United States, and China, have also been "accused of launching similar attacks on adversaries." For example, China has been accused of attacking the U.S. Department of Defense "as well as government agencies in France, Germany, South Korea, and Taiwan."[3] One author lists international attacks dating back to 1999. That year hackers from Serbia attacked NATO "in retaliation for NATO's military intervention in Kosovo" and Chinese hackers attacked U.S. government websites after the bombing of the Chinese embassy.[4] John Aquilla, an associate professor of defense analysis at the Naval Postgraduate School, implied in a Frontline interview that the U.S. also used a form of cyber attack to affect the Serbian integrated air defense system (IADS) during that conflict to gain air superiority.[5] The international community has not failed to notice the dangers associated with cyber warfare.

After the 2007 attacks on Estonia, seven NATO nations established the Cooperative Cyber Defence Centre of Excellence.[6] However, this endeavor falls far short of an international agreement on the conduct of cyber warfare. The purpose of the organization is to "conduct research and training on cyber warfare."[7] It is a start towards limited international cooperation but it does not define acts of cyber warfare nor does it establish agreements on limitations of attacks or layout consequences for violators. The United Nations also has an organization with many member nations addressing some of the issues as well. The International Multilateral Partnership Against Cyber Threats (IMPACT) is an offshoot of the UN's International Telecommunication Union. A long list of nations from Afghanistan to Zambia[8] participate and their stated mission is "… bringing together governments, academia, industry leaders and cybersecurity experts to enhance the global community's capacity to prevent, defend against and respond to cyber threats." [9] Like NATO's endeavor, this initial step by the UN lacks promissory signatures of two or more nation states to establish international law regarding cyber warfare. There are several reasons such a treaty is difficult to obtain.

Various characteristics of cyber warfare create obstacles to penning international treaties. The first obstacle is defining what acts constitute an act of war. Panelists at the January 2010 State of the Net conference were not even able find consensus "on what exactly constitutes an act of war in cyberspace."[10] Is cyber espionage an act of war? Must there be physical damage to constitute an act of war or is it sufficient to impact the economy? If causing economic impact is an act of war, what is the monetary threshold? Another tremendous obstacle is attribution. It is very difficult to prove who originated the attack. In a time of computer zombies and botnets an attack may appear to come from Nation A but state or non-state actors from Nation B may be the true perpetrators exploiting weaknesses in Nation A's networks. Likewise, if it is so difficult to prove an attack was not a form of non-state terrorism, how can any nation be held accountable? The final significant obstacle is verifying compliance. In nuclear arms treaties, inspectors could inspect facilities, count missiles and warheads, and monitor destruction of weapons. How can one nation verify another's compliance? Any computer can be used and computers are more proliferated around the world than any other weapon. With so many cyber weapons around the world, it is time to codify international law.

The Bipartisan Policy Center (BPC) made this point clear earlier this year in a cyber warfare exercise designed to conduct a simulation "through the lens of a notional National Security Council (NSC) meeting convened to advise the president on how the federal government should respond to the crisis..."[11] The BPC's Cyber ShockWave exercise differed significantly from previous exercises coordinated by the Dept of Homeland Security (DHS) called Cyber Storm. Cyber Storm exercises are "designed to test communications, policies and procedures in response to various cyber attacks and to identify where further planning and process improvements are needed."[12] In Cyber Storm, government agencies, telecommunication representatives, and international partners look at attacks to consider methods of defense. While that is valuable, it is limited in scope to the tactical issues of cyber warfare. On the other hand Cyber ShockWave was conducted "by former top-ranking national security officials"[13] who focused on issues of policy, law, and international attribution. The Washington Post summary of Cyber ShockWave states, "A massive cyber attack has turned the cell phones and computers of tens of millions of Americans into weapons to shut down the Internet. A cascading series of events then knocks out power for most of the East Coast amid hurricanes and a heat wave."[14] It addressed the tough issues including international actors, government authority over private telecommunications, and U.S. infrastructure vulnerabilities. Cyber ShockWave demonstrated again that the U.S. is ill prepared.

One perspective of note on Cyber ShockWave comes from former Department of Homeland Security Secretary Michael Chertoff. To provide perspective on cyber warfare he wrote, “cyber warfare is a major national security issue — protecting the security and freedom of our networks is as critical as protecting freedom of the seas and space.”[15] The comparison to seas and space is particularly interesting because the international community has already signed treaties regarding the sea and space domains. He goes on to draw a parallel to another issue for which international treaties exist. He stated the exercise clearly showed the government should “formulate a strategy for deterrence and response to state-sponsored cyber attacks that parallels the national security strategies we developed for dealing with nuclear threats during the Cold War.”[16] While Chertoff called for U.S. policy similar to nuclear policies, the parallel also extends to international treaties. Like U.S. nuclear policy, a clear U.S. cyber policy may deter some actors from cyber strike. However, nuclear treaties provide for international cooperation to further reduce the threat of nuclear strikes. International treaties for cyber warfare would provide the framework for similar cooperation. Chertoff did not directly call for treaties but his conclusions strongly support the argument for a treaty providing international law and international cooperation.

The first step is a first draft. The U.S. should look to its strongest allies to lay down the first agreements. Rather than try to tackle the difficult issues with an argumentative adversary, laying the framework for larger international agreements with close allies can set the stage for including wider international participation. Furthermore, the U.S. and partners should not get hung up on the obstacles described above. If disagreements arise on defining an act of war, the signatories can start with a simple concept. Any cyber attack from a nation-state that intentionally causes damage, injury, or death is an act of war. Such acts from non nation-state actors can be considered a crime as terrorist acts often are. In the case of a severe attack by a non-state actor, if a nation is not willing to cooperate in apprehending the responsible parties, their refusal may be grounds for war. When Al-Qaeda attacked the U.S. in 2001 many nations backed the U.S. actions against the ruling Taliban in Afghanistan to address the threat. A parallel policy can be instituted for treaties. Signatories can further agree to institute national laws to require ISPs and telecommunication hubs to store network traffic logs for an agreed minimum period to aid investigations. Along with the logs, the agreement can include regular inspections of the logs and network infrastructure. Providing open access to the logs and network infrastructure allows the signatories to maintain a more complete network map that would aid in tracing attacks. These initial agreements provide a foundation for evolution in further agreements much like nuclear agreements evolved in successive treaties.

Both history and exercises have demonstrated the world cannot afford to wait any longer. Cyber attacks have occurred for years and threaten to impact nations in many ways from simple denial of access to destruction of infrastructure. In the past nations have signed treaties to regulate warfare and halt arms races to avoid catastrophic consequences to populations. It is time to overcome the obstacles. Agreements can start with a compromise in defining what constitutes attacks and grow on the international cooperation already present in the UN and NATO. In the past governments have acted to ensure peace for their populations as well as established international laws for the conduct of war. It is time for the international community to include this advance in warfare into those laws.

Endnotes

[1] Bruno, “The Evolution of Cyber Warfare.”
[2] Ibid.
[3] Ibid.
[4] Corin, “Some Key Events In The History of Cyber Warfare.”
[5] Frontline, “Cyberwar!”
[6] NATO, “NATO Opens New Centre of Excellence on Cyber Defence.”
[7] Ibid.
[8] IMPACT, “Countries.”
[9] IMPACT, “About Us.”
[10] Gross, “Experts: US gov't needs to prepare for cyberwar.”
[11] Chertoff, “Cyber ShockWave exposed missing links in U.S. security.”
[12] DHS, “Factsheet: Cyber Storm Exercise.”
[13] Nakashima, “War game reveals U.S. lacks cyber-crisis skills”
[14] Ibid.
[15] Chertoff, “Cyber ShockWave exposed missing links in U.S. security.”
[16] Ibid.

Bibliography

Bruno, Greg. "The Evolution of Cyber Warfare." *Council on Foreign Relations Website.* 27 February 2008. http://www.cfr.org/publication/15577/evolution_of_cyber_warfare.html

Chertoff, Michael. "Cyber ShockWave exposed missing links in U.S. security." 10 March 2010. http://gcn.com/articles/2010/03/15/commentary-chertoff-cyber-shockwave.aspx

Corrin, Amber. "Some Key Events In The History of Cyber Warfare." *Federal Computer Week Website.* 15 October 2009. http://fcw.com/articles/2009/10/19/feat-dod-cyber-timeline.aspx

Department of Homeland Security. "Fact Sheet: Cyber Storm Exercise." *DHS Website. http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm*

Frontline Website. "Cyberwar!" http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html

Gross, Grant. "Experts: US gov't needs to prepare for cyberwar." *The industry Standard Website.* http://www.thestandard.com/news/2010/01/27/experts-us-govt-needs-prepare-cyberwar

International Multilateral Partnership Against Cyber Threats. "About Us." *IMPACT Website*. http://www.impact-alliance.org/about_us.html

International Multilateral Partnership Against Cyber Threats. "Countries." *IMPACT Website*. http://www.impact-alliance.org/countries.html

Nakashima, Ellen. "War game reveals U.S. lacks cyber-crisis skills." *The Washington Post Website.* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/16/AR2010021605762.html

North Atlantic Treaty Organization. "NATO Opens New Centre of Excellence on Cyber Defence." *NATO Website.* http://www.nato.int/cps/en/natolive/news_7266.htm?selectedLocale=en